⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－24384

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)2月1日
G 06 K 17/00		T－6711－5B	
E 05 B 49/00		6637－2E	
G 06 F 1/00	370	7157－5B	
15/21	340	Z－7230－5B	審査請求　有　発明の数　5　（全31頁）

㊹発明の名称　別個の時間動作装置を同期させる装置および方法

㉑特　願　昭61－283041

㉒出　願　昭61(1986)11月27日

優先権主張　㉜1985年11月27日㉝米国(US)㉛802579

㉗発明者　ケネス・ピー・ウエイス　アメリカ合衆国マサチユーセツツ州02109，ボストン，ドワイト・ストリート　15

㉑出願人　セキユリテイ・ダイナミツクス・テクノロジーズ・インコーポレーテツド　アメリカ合衆国マサチユーセツツ州02140，ケンブリツジ，マサチユーセツツ・アベニユー　2067

㉔代理人　弁理士　湯浅　恭三　外5名

明　細　書

1　発明の名称

別個の時間動作装置を同期させる装置および方法

2　特許請求の範囲

1．時間に従って個々のクロック装置により定義される動的変数に基いて個々のコンピュータにより生じる予測不能コードを比較して突合せを行なうシステムにあって，前記動的変数の時間的定義を同期させる装置において，

ある予め定めたアルゴリズムに従って第1の予測不能コードを計算する第1のコンピュータを設け，該アルゴリズムは第1の動的変数および一義的な静的変数に基いて前記第1の予測不能コードを生成し，

前記静的変数が前記アルゴリズムに対し入力される第1の時間間隔に従って前記第1の動的変数を自動的に定義する第1のクロック装置を設け，前記第1の時間間隔は第1の予め定めた持続期間を有し，

前記の予め定めたアルゴリズムに従って2つ以上の第2の予測不能コードを計算する第2のコンピュータを設け，該アルゴリズムは前記の2つ以上の第2の動的変数と一義的な静的変数に基いて前記第2の予測不能コードを生成し，

前記静的変数が前記第2のコンピュータのアルゴリズムに対し入力される第2の時間間隔の2つ以上のセルに従って前記の2つ以上の第2の動的変数を自動的に定義する第2のクロック装置を設け，該第2の時間間隔は1つの予め定めた持続期間を有する1つの中心の時間セルと，該中心の時間セルの境界をなす1つ以上の時間セルとからなり，各境界の時間セルはある予め定めた持続期間を有し，

前記第1の予測不能コードを前記第2の予測不能コードと比較して整合状態を判定する装置と，

前記第2の予測不能コードの1つに対する前

記第１の予測不能コードの比較および突合せと同時に、前記第１のクロック装置と前記第２のクロック装置とを自動的に同期させる装置とを設けることを特徴とするシステム。

２．前記中心の時間セルが、前記の一義的な静的変数が前記第２のクロック装置により定義される如く第２のコンピュータに対して入力される日付と時分とからなることを特徴とする特許請求の範囲第１項記載のシステム。

３．前記の境界の時間セルが、前記の中心の時間セルの直前の日付と時分とからなることを特徴とする特許請求の範囲第２項記載のシステム。

４．前記同期装置が、

整合する第２の予測不能コードを生成することができる中心の時間セルと境界の時間セルとの間の時間的差をカウントするカウント装置と、

該カウント装置によりカウントされる連続する時間的差を加算するため前記カウント装置と結合された加算装置と、

該加算装置の出力を格納するため加算装置との時間的差をカウントするため前記第２の格納装置と結合された第２のカウント装置と、

ある選択された値により前記第２のカウント装置によりカウントされた時間的差を除し、出力を第１の窓開放番号として定義するため前記第２のカウント装置と結合された除算装置と、

前記第１の窓開放番号により定義される如き選択された数の前記境界のセルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第２の予測不能コードを計算するため前記除算装置および前記比較装置と結合された窓開放装置とを含むことを特徴とする特許請求の範囲第５項記載のシステム。

８．前記同期装置が更に、

前記第２のクロック装置の再セッティングを検出するため第２のクロック装置と結合された検出装置と、

ある選択された第２の窓開放番号として前記第２のクロック装置の検出された再セッティングの発生を定義してこれを格納するため前記検出装置と結合された第３の格納装置と、

前記第２の窓開放番号により定義される如き別の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第２の予測不能コードを計算するため前記第３の格納装置と結合された第２の窓開放装置とを含むことを特徴とする特許請求の範囲第７項記載のシステム。

９．前記第１のコンピュータが、前記アルゴリズムが動作装置と共に包含された揮発性の動的メモリーに格納されるマイクロプロセッサを含み、前記動作装置は、割込みされる時、少なくとも前記アルゴリズムおよび静的変数を含む全てのデータを破壊することを特徴とする特許請求の範囲第８項記載のシステム。

10．前記第１のコンピュータと前記第１のクロック装置とがクレジット・カードと略々同じサイズのカードに内蔵されることを特徴とする特許請求の範囲第９項記載のシステム。

11．前記第２のコンピュータのアルゴリズムが、

前記比較装置による最も後の比較および突合せの日付を格納するため前記比較装置と結合された第２の格納装置と、

格納された前記日付と、前記第２のコンピュータに対するその時のエントリの日付との間

動作装置と共に包含された隠発性の動的メモリーに格納され、前記動作装置は、割込みされる時、少なくとも前記アルゴリズムおよび前記静的変数を含む全てのデータを破壊することを特徴とする特許請求の範囲第10項記載のシステム。

12. 動的変数が整合する時コードが整合する時間に従って個々のクロック装置により定義される動的変数に基いて別個のコンピュータにより生成される予測不能コードを比較する方法であって、前記動的変数の時間の定義を同期する方法において、

ある静的変数をある予め定めたアルゴリズムを含む第1のコンピュータに対して入力し、

該第1のコンピュータのアルゴリズムを用いて、前記静的変数に基いて第1の予測不能コードと、第1のクロック装置に従って前記入力ステップが生じた第1の時間間隔により定義される第1の動的変数とを計算し、

前記静的変数と前記第1の予測不能コードとを前記の予め定めたアルゴリズムを独立的に含む第2のコンピュータに対して入力し、

前記第2のコンピュータのアルゴリズムを用いて、前記静的変数と、前記入力ステップが第2のクロック装置に従って生じた第2の時間間隔の2つ以上のセルにより定義される2つ以上の第2の動的変数とを独立的に計算し、前記第2の時間セルは1つの中心の時間セルと1つ以上の境界の時間セルとからなり、

前記第1の予測不能コードを前記第2の予測不能コードと比較して整合状態を判定し、

前記第2の予測不能コードの1つに対する前記第1の予測不能コードの比較および突合せと同時に、前記第1のクロック装置と前記第2のクロック装置を同期させるステップとからなることを特徴とする方法。

13. 前記同期ステップが、

整合する第2の予測不能コードを生成し得る1つの中心の時間セルと1つの境界の時間セルとの間の時間的差をカウントし、

該カウント・ステップにおいてカウントされた連続する時間的差を加算し、

加算された連続する時間的差を格納し、

加算された前記連続時間的差だけ前記中心および境界の時間セルをシフトするステップを含むことを特徴とする特許請求の範囲第12項記載の方法。

14. 前記同期ステップが更に、

整合状態の最も後の比較および判定の日付を格納し、

前記の格納された日付とその時の第2のコンピュータへのエントリの日付との間の時間的差をカウントし、

ある選択された値により前記日付の差をカウントする前記ステップの間カウントされた差を除して、出力を第1の窓開放番号として定義し、

前記第1の窓開放番号により定義される如き前記の選択された数の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第2の予測不能コードを計算するステップを含むことを特徴とする特許請求の範囲第13項記載の方法。

15. 前記同期ステップが更に、

前記第2のクロック装置の再セッティングを検出し、

前記第2のクロック装置の検出された再セッティングの発生第2の選択された窓開放番号として定義して格納し、

前記第2の窓開放番号により定義される如き別の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第2の予測不能コードを計算するステップを含むことを特徴とする特許請求の範囲第14項記載の方法。

16. 前記中心および境界の時間セルが持続期間において1分となるように選択されることを特徴とする特許請求の範囲第12項記載の方法。

17. 予測不能コードの電子的な生成および比較を行なう装置において、

ある予め定めたアルゴリズムに従って第1の予測不能コードを計算する第1の装置を設け、該

第1の計算装置は、一義的な静的変数を前記の予め定めたアルゴリズムに対して入力する第1の装置を含み、

前記第1の入力装置が付勢される時間間隔に従って第2の動的変数を自動的に定義する第1の装置を設け、該第1の自動定義装置は、前記第1の計算装置の前記の予め定めたアルゴリズムに前記第1の動的変数を自動的に使用できるようにする装置を含み、

前記の予め定めたアルゴリズムに従って第2の予測不能コードを計算する第2の装置を設け、該第2の計算装置は、前記の一義的な静的変数を前記の予め定めたアルゴリズムに対して入力する第2の装置を含み、

前記第2の入力装置が付勢される時間間隔に従って第2の動的変数を自動的に定義する第2の装置を設け、該第2の自動定義装置は、前記第2の計算装置の前記の予め定めたアルゴリズムに前記第2の動的変数を自動的に使用できるようにする装置を含み、

前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を設けることを特徴とする装置。

18. 前記第1の計算装置が、前記の予め定めたアルゴリズムを実施する第1のプログラムでロードされた第1のコンピュータを含むことを特徴とする特許請求の範囲第17項記載の装置。

19. 前記第1のコンピュータが、前記第1のプログラムが動作装置と共に内蔵された揮発性の動的メモリーに格納され、前記動作装置は、割込みされる時、少なくとも前記プログラムと前記静的変数とを含む全てのデータを破壊することを特徴とする特許請求の範囲第18項記載の装置。

20. 前記第1の動的変数を自動的に定義する前記第1の装置が、前記の予め定めたアルゴリズムに前記第1の動的変数を自動的に使用できるようにして、前記静的変数が入力される時間間隔に従って前記第1の動的変数を定義する時計装置を含むことを特徴とする特許請求の範囲第19項記載の装置。

21. 前記第2の計算装置が、前記第1のコンピュータから離れた接近管理装置を含み、該接近管理装置は、前記の予め定めたアルゴリズムを実施する第2のプログラムがロードされていることを特徴とする特許請求の範囲第20項記載の装置。

22. 前記第2の動的変数の自動定義装置が、前記接近管理装置の前記の予め定めたアルゴリズムに前記第2の動的変数を自動的に使用可能にして、前記静的変数が入力される前記時間間隔に従って前記第2の動的変数を定義する時計装置を含むことを特徴とする特許請求の範囲第21項記載の装置。

23. 前記第2のプログラムが動作装置と共に内蔵された揮発性の動的メモリーに維持され、前記動作装置は、割込みされる時、前記プログラムと前記第2のプログラムに入力される静的変数とを含む全てのデータを破壊することを特徴とする特許請求の範囲第21項または第22項に記載の装置。

24. 前記第2の計算装置と前記比較装置とに対する前記静的変数および前記第1の予測不能コードの即時の順次通信をそれぞれ行なう装置を更に設けることを特徴とする特許請求の範囲第17項記載の装置。

25. 前記第2の計算装置と前記比較装置とに対する前記静的変数および前記第1の予測不能コードの即時の順次通信をそれぞれ行なう装置を更に設けることを特徴とする特許請求の範囲第21項記載の装置。

26. 前記第2の計算装置が、前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を含むことを特徴とする特許請求の範囲第24項記載の装置。

27. 前記第2の計算装置が、前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を含むことを特徴とする特許請求の範囲第25項記載の装置。

28. 前記第1のコンピュータと前記第1の自動定義装置とが、クレジット・カードと略々同じサイズのコードに内蔵されることを特徴とする特許請

求の範囲第19項、第21項、第24項または第25項のいずれかに記載の装置。

29. 前記接近管理装置が携帯可能であることを特徴とする特許請求の範囲第22項記載の装置。

30. 前記静的変数を前記第1のコンピュータの予め定めたアルゴリズムに対して自動的に入力する装置を更に設けることを特徴とする特許請求の範囲第19項記載の装置。

31. 前記第1の予測不能コードを個々に検出する装置を更に設けることを特徴とする特許請求の範囲第30項記載の装置。

32. 予測不能コードを生成して比較する方法において、

静的変数を予め定めたアルゴリズムを含む第1のコンピュータに対して入力し、

該第1のコンピュータの前記アルゴリズムを用いて、前記静的変数と、前記入力ステップが生じた時間間隔により定義される第1の動的変数とに基いて第1の予測不能コードを計算し、

前記静的変数を前記の予め定めたアルゴリズムを独立的に含む接近管理装置に対し入力し、

前記接近管理装置のアルゴリズムを用いて、前記静的変数と前記入力ステップが生じた時間間隔により定義される第2の動的変数とに基いて、第2の予測不能コードを独立的に計算し、

前記接近管理装置のアルゴリズムを用いるステップと前記第1の予測不能コードのアルゴリズムを用いるステップにおいて計算される予測不能な数字コードを比較するステップとからなり、

前記第1の動的変数と前記第2の動的変数は、前記接近管理装置のアルゴリズムを用いるステップと前記第1の予測不能コードのアルゴリズムを用いるステップが同じ時間間隔内に生じる時にのみ前記アルゴリズムから整合するコードを生成するように等しいことを特徴とする方法。

33. 前記第1のコンピュータのアルゴリズムを用いるステップが、前記静的変数の前記第1のコンピュータに対する入力に応答して、前記第1の動的変数を前記第1のコンピュータのアルゴリズムに対し自動的に入力する時計装置により前記第1の動的変数を定義するステップを含むことを特徴とする特許請求の範囲第32項記載の方法。

34. 前記第1のコンピュータが、割込みされる時前記プログラムおよび静的変数を含む全てのデータを破壊する動作装置と共に内蔵された揮発性の動的メモリーに格納された前記アルゴリズムを含む第1のプログラムを有するマイクロプロセッサを含むことを特徴とする特許請求の範囲第33項記載の方法。

35. 前記静的変数を入力するステップが更に、前記入力ステップが生じると同じ時間間隔内で前記第1と第2の予測不能コードを比較する装置に対し前記第1の予測不能コードを通信するステップを更に含むことを特徴とする特許請求の範囲第34項記載の方法。

36. 前記接近管理装置のアルゴリズムを用いる前記ステップが更に、前記静的変数の前記接近管理装置に対する入力に応答して、前記静的変数と、前記接近管理装置のアルゴリズムに対し前記第2の動的変数を自動的に入力する時間間隔により定義される第2の動的変数とに基いて、第2の予測不能コードを独立的に計算するステップと含むことを特徴とする特許請求の範囲第33項または第35項に記載の方法。

37. 前記接近管理装置のアルゴリズムを用いる前記ステップが、前記静的変数を入力する前記ステップの実施に応答して、前記第2の動的変数を前記第2のコンピュータに対して自動的に入力する時計装置により前記第2の動的変数を定義するステップを含むことを特徴とする特許請求の範囲第35項記載の方法。

38. 前記静的変数を入力する前記ステップが、前記マイクロプロセッサにより自動的に実施されることを特徴とする特許請求の範囲第37項記載の方法。

39. 第1の機構が、一義的な静的変数と動的変数の双方に応答して、ある予め定めたアルゴリズムに従って第1の予測不能コードを生成し、第2の機構が、前記の一義的な静的変数と前記第1の動的変数と対応する第2の動的変数との双方に応答

して、前記の予め定めたアルゴリズムに従って第２の予測不能コードを生成し、２つの予測不能コードを比較する装置を含む形式の機密保護システムにおいて使用される携帯可能な手に保持される計算兼表示装置であって、第１の機構を形成する装置において、

前記アルゴリズムを内部に予めプログラムされたプロセッサと、

前記アルゴリズムを知るため前記プログラムに対する接近を行おうとすると前記プロセッサに格納された前記プログラムを消去させる装置と、

各装置内に一義的な静的変数を格納する装置とを設け、該静的変数は第２の機構と共に使用されるための２つの装置が同じ静的変数を格納することがないように選択され、

時間と共に変化する動的変数を生成する装置を設け、該装置は実質的に同じ時間間隔において前記第２の機構において生成されたものと同じ動的変数を生成するようになっており、

前記の格納された一義的な静的変数とその時生成された動的変数とを前記プロセッサに対して加える装置と、

前記プロセッサによりその時生成されつつある予測不能コードを視覚的に表示する装置とを設けることを特徴とする装置。

40. 前記プロセッサを内部に密閉したクレジット・カードのサイズのカードの形態を有することを特徴とする特許請求の範囲第39項記載の装置。

41. 前記カードが、約84mm（3.3 インチ）の長さと約53mm（2.1 インチ）の巾と約1.8 mm（0.07インチ）より薄い厚さとを有することを特徴とする特許請求の範囲第40項記載の装置。

42. 前記の視覚的に表示する装置が液晶ディスプレイであることを特徴とする特許請求の範囲第39項記載の装置。

43. 時間と共に変化する動的変数を生じる前記装置が電子的なクロック・ゼネレータであることを特徴とする特許請求の範囲第39項記載の装置。

3　発明の詳細な説明

（関連出願）

本願は、1984年11月30日出願のKenneth Weissの米国特許出願第 676,826号の一部継続出願である。

（発明が属する技術分野）

本発明は、変更可能で予測不能なコードの電子的な生成、および装置またはシステムの許可された個人即ちユーザを確実に識別する目的のためかかるコードの検証および比較を行ない、然る後保護されたシステムまたは施設に対する特に許された取引きまたは接近を実施するため許可を与える装置および方法に関する。

（従来の技術およびその問題点）

選ばれた許可人員を除く全ての人員がある定義された取引き（信用の許与の如き）を実施しあるいは電子的装置その他のシステム、施設またはデータに対する接近を得ることができないようにする必要（以下本文では、「接近の許可」という）がしばしば生じる。不当な許可または接近を阻止する従来の方法は、前記のデータ、施設に対する接近、または彼の如き物理的な一義的な装置を保持する者または固定された即ち予測可能な（以下本文では「固定」という）秘密コードを知る者に対する取引きを制限する装置を含むのが一般的である。このような選択的な許可または接近を得る手段として固定されたコードまたは一義的な物理的な装置に依存することに特有の問題は、偽の許されないユーザがこのような許可または接近を得るため固定コードまたは一義的な装置を手に入れるだけでよいということである。固定コードの典型的な事例には、コンピュータ・データの検索サービスの顧客に対し発行されるコード番号、ユーザ番号またはパスワードが含まれる。

（問題を解決する手段）

本発明の主な目的は、しばしば相互に同期時期から外れ得る個々の装置において生じるデータおよび時間の情報に基いて独立的に生成される時間に依存する予測できないコードの発生を同期させることにある。本発明の更に別の目的は、ユーザ

に固有でありかつユーザの介入なしに周期的に変更するが許可または接近を何時でも与えるための識別の検証が容易に可能な手段を提供する識別コードを生成する実際的な試みを提供することになる。

（発明の要約）

本発明は、前以て知らされずかつ固定秘密コードを使用する装置の許可されたユーザにとってさえ保全システムの管理部署外では知ることができない固定コード、可変データおよび予め定めたアルゴリズムを用いて識別コードを周期的に生成することにより、秘密の「固定」コードをコピーするか他の方法で不当に使用する者に許される比較的容易な接近を排除するものである。予め定めたアルゴリズムは、常に新しい一義的かつ検証可能な予測できないコードを生成するが、このコードは予め定めたアルゴリズムによって固定データおよび日付け（曜日を含む）の如き少なくとも1つの動的変数から得られる。アルゴリズムにより処理される時この動的変数における経常的な変化は、結果として常に変化する予測できないコードの生成をもたらすことになる。

本発明によれば、時間に従って個々のクロック機構により規定される動的変数に基いて別個のコンピュータにより生じる予測できないコードを比較して整合するためのシステムにおいて、動的変数の時間的定義を同期するための装置が提供され、その構成は、予め定めたあるアルゴリズムに従って第1の予測できないコードを計算するための第1のコンピュータを設け、該アルゴリズムは第1の動的変数および一義的な静的変数に基いて第1の予測できないコードを生成し、静的変数がアルゴリズムに入力される第1の時間間隔に従って第1の動的変数を自動的に定義する第1のクロック機構を設け、該第1の時間間隔は第1の予め定めた持続期間を有し、前記の予め定めたアルゴリズムに従って2つ以上の予測できないコードを計算する第2のコンピュータを設け、該アルゴリズムは前記の2つ以上の動的変数および一義的な静的変数に基いて前記第2の予測できないコードを生成し、前記静的変数が前記第2のコンピュータのアルゴリズムに入力される第2の時間間隔の2つ以上のセルに従って前記の2つ以上の動的変数を自動的に定義する第2のクロック機構を設け、前記第2の時間間隔は予め定めた持続期間を有する1つの中心時間セルとこの中心時間セルの境界にある1つ以上の時間セルとからなり、各境界の時間セルはある予め定めた持続期間を有し、前記第1の予測できないコードを前記第2の予測できないコードと比較して整合状態を決定し、前記第2の予測できないコードの一方に対する前記第1の予測できないコードの比較および突合せと同時に前記第1のクロック機構と第2のクロック機構を自動的に同期させる機構を設けてなる。

前記の中心時間セルは、一般に、一義的な静的変数が第2のクロック機構により定義される如き第2のコンピュータに対し入力される日付けおよび時分からなり、前記の境界の時間セルは中心のセルの直前の日付けおよび時分からなる1つの時間セルからなっている。

同期させる機構は、中心時間セルと境界の時間セルとの間の時間の差をカウントしてこれから第2の突合せする予測できないコードを生成できるカウント機構と、このカウント機構によりカウントされた時間の連続的な差を加算するため前記カウント機構と結合された加算機構と、この加算機構の出力を格納するため加算機構と結合された格納機構と、この格納機構に格納された前記加算機構の出力により中心の時間セルと境界の時間セルをシフトするため格納機構と結合されたシフト機構とからなることが望ましい。

境界の時間セルは、前記の中心の時間セルの直前のある選択された数のセルと、中心の時間セルの直後のある選択された数のセルとからなり、中心および境界の時間セルは典型的には持続期間が1分となるように選択される。

前記同期機構は更に、最も後の比較の日付けを格納して比較機構による突合せを行なうためこの比較機構と結合された第2の格納機構と、格納さ

れた日付と第2のコンピュータに対するその時のエントリの日付との間の時間的な差をカウントするため前記第2の格納機構と結合された第2のカウント機構と、第2のカウント機構によりカウントされた時間的差をある選択された値で除して第1の窓開放番号として出力を定義するため第2のカウント機構と結合された除算機構と、この第1の窓開放番号により定義される如き選択された数の境界の時間セルの直前と直後の多数の別の境界の時間セルに基いてこれと同数の別の予測できないコードとして計算するため前記除算機構および前記比較機構と結合された窓開放機構とからなることが望ましい。

前記同期機構は更に、前記第2のクロック機構の再セッティングのため第2のクロック機構と結合された検出機構と、選択された第2の窓開放番号として前記第2のクロック機構の検出された再セッティングの発生を定義して格納するため前記検出機構と結合された第3の格納機構と、前記第2の窓開放番号により定義される如き別の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いてこれと同数の別の第2の予測できないコードを計算するため前記第3の格納機構と結合された第2の窓開放機構とを含むことが最も望ましい。

前記第1のコンピュータは、典型的には、割込みが生じる時少なくともアルゴリズムと静的変数を含む全てのデータを破壊する動作機構を内蔵した揮発性の動的メモリーに前記アルゴリズムが格納されるマイクロコンピュータを含む。

更に望ましくは、前記第2のコンピュータのアルゴリズムは、割込みが生じる時少なくともアルゴリズムと静的変数を含む全てのデータを破壊する動作機構を内蔵した揮発性の動的メモリーに格納される。

動的変数が整合する時コードが整合する時間に従って個々のクロック機構により定義される動的変数に基いて別個のコンピュータにより生じる予測できないコードを比較する方法においては、下記のステップからなる動的変数の時間的定義を同期させる方法もまた提供される。即ち、ある予め定めたアルゴリズムを含む静的変数を第1のコンピュータに対して入力し、この第1のコンピュータのアルゴリズムを用いて、前記静的変数に基き第1の予測できないコードを、またある第1の時間間隔により定義される第1の動的変数を計算し、前記入力ステップは第1のクロック機構に従って生じ、前記静的変数と第1の予測できないコードを前記の予め定めたアルゴリズムを独立的に含む第2のコンピュータに対して入力し、該第2のコンピュータのアルゴリズムを用いて前記静的変数に基き2つ以上の第2の予測できないコードを、また第2の時間間隔の2つ以上のセルにより定義される2つ以上の動的変数を独立的に計算し、前記の入力ステップは第2のクロック機構に従って生じ、前記第2の時間間隔は1つの中心の時間セルと1つ以上の境界の時間セルからなり、前記第1の予測できないコードを前記第2の予測できないコードと比較して整合状態を決定し、前記第2の予測できないコードの一方に対する前記第1の予測できないコードの比較および突合せと同時に前記第1のクロック機構と前記第2のクロック機構を同期させるステップからなる。

この同期ステップは、これからある突合せる第2の予測できないコードが生成できる1つの中心の時間セルと1つの境界の時間セルとの間における時間的差をカウントし、このカウント・ステップの間にカウントされた連続する時間的差を加算し、この加算された連続する時間的差を格納し、かつこの加算された連続的な時間的差だけ前記の中心および境界の時間セルをシフトするステップからなることが望ましい。

更に望ましくは、前記の同期ステップは更に、最も後の比較および突合せの決定の日付を格納し、この格納された日付と前記第2のコンピュータに対するその時のエントリの日付との間の時間的差をカウントし、選択された値によりカウントされた日付の差を除して出力を第1の窓開放番号として定義し、この第1の窓開放番号により定義

されたものの選択された数の境界の時間セルの直後と直前の別の隣時間セルに基いてこれと同数の別の第２の予測できないコードを計算するステップからなる。

更に望ましくは、前記の同期ステップは更に、前記第２のクロック機構の再セッティングを検知し、第２の選択された窓開放番号として前記第２のクロック機構の検出された再セッティングの発生を定義して格納し、前記第２の窓開放番号により定義された如き前記の別の境界の時間セルの直前と直後の別の境界の時間セルに基きこれと同数の別の第２の予測できないコードを計算するステップを含む。

第１のコンピュータと、接近管理装置と、ホスト・コンピュータと、比較装置のいずれかまたは両方に含まれる揮発性の動的メモリーは、望ましくは、予め定めたアルゴリズム、システムの動作プログラム、コードの比較および突合せプログラム等の全てのプログラムを格納して維持し、前記の揮発性の動的メモリーは更に望ましくは、固定コード、結果のコード、動的変数等の全てのデータおよび動作の結果を格納し、維持しかつこれを使用することを可能にする。

他の目的、特徴および長所については、図面と関連して本発明の望ましい実施態様の以下の詳細な記述を照合すれば明らかになるであろう。

〔実施例〕

本発明によれば、有資格者は、典型的に個人に一義的な番号である第１図、第１Ａ図、第２図および第３図の固定された秘密コード即ちカードのシード10が与えられる。第２図のクレジット・カードまたは銀行／キャッシュ・カード20の場合、この番号10は、もし資格のあるカードの持主が番号を忘れた場合に、カードまたは固定コード10の他の恒久的に印刷されたものを照合することにより迅速に検索することができるように、カード自体に印刷することができる。固定コード／カード・シード10が恒久的な印刷形態もしくは本発明の装置と密着する形態で提供される場合は、この固定コード10の別の部分、所謂ピン45（各人の識別番号）も設けられることが望ましいが、これは資格のあるユーザを固定コード／カード・シード10の不正使用に対して更に保護するためユーザが記憶する。あるいはまた、固定コード／カード・シード10またはピン45は許可または接近を許す関管轄部署により発行される許可されるターミナルを識別するため使用することができる。

このような固定および（または）記憶コード（一般に、第３図のピン45即ち個人の識別番号）は、接近管理モジュール（ＡＣＭ）またはホスト・コンピュータ50（第１図、第１Ａ図、第３図）に対して、一義的な静的変数10と共に入力され、第３図のホストまたはＡＣＭのメモリー内に一時的に格納される（第３図のステップ100）。

望ましくは、一旦カード・シード10およびピン45がホストまたはＡＣＭ50に入力されると、整合状態となるかどうかを判定するため、その各々は個々に許可されたカードのピンのライブラリと比較され（第３図のステップ110）、またホストまたはＡＣＭメモリーに格納された許可されたカード・シードのライブラリと比較される（第３図のステップ120）。もしユーザがホストまたはＡＣＭに入力するピン45またはカード・シード10のいずれかが整合状態を生じなければ、許可または接近は拒絶され、カードのユーザは再び接近または許可を得るため初めからやり直さなければならない。

最終的にはユーザに許可もしくは接近を許与することになる予測不能コード40（第１図乃至第３図）を生成するためには、固定コード即ちシード10および（または）ピン45はシード10および（または）ピン45を静的変数として維持する予め定めたあるアルゴリズムに対して入力されなければならない。このアルゴリズムは、典型的には、ユーザに対して計算機20（第２図）の形態で与えられ、これは予め定めたアルゴリズムを実施するためのプログラムがロードされている。この計算機20は、望ましくは電子計算機からなり、更に望ま

しくは予め定めたアルゴリズムの諸機能を格納し実施するため充分な最の障発性の動的メモリーを備えマイクロプロセッサからなる。このコンピュータ20は、クレジット・カードの体裁とおおよその寸法を有するカード20（第２図）内に提供されることが最も望ましい。

このようなクレジット・カード・サイズのコンピュータ20（第２図）はまた、アルゴリズムにより生成される最終的な予測不能コード40（第３図において、「カードの結果のコード」として示される）を表示するための従来周知の液晶ディスプレイ44を含むことが望ましい。このように生成された予測不能コード40は、ホスト・コンピュータまたはＡＣＭ50（第１図、第１Ａ図、第３図）に対して実際に入力するため、ユーザが目で見ることができる。第２図に示されるように、カード・コンピュータ20の望ましい態様は、約84mm（3.3インチ）の長さＬと、約53mm（2.1 インチ）の巾Ｗと、約1.8 mm（0.07インチ）より薄い厚さＤを有する。マイクロプロセッサ20に第１の予測不能コード40の視覚的な表示のため液晶ディスプレイ45を設けることに加えて、あるいはその代りに、コンピュータ20は第１の予測不能コード40（即ち、カードの結果のコード）および（または）ピン45をＡＣＭまたはホスト50により機械で読取る装置を含めてもよく、あるいは第１の予測不能コード40を個人的に検知するための音響を生じるかまたは他の手段を含めることもできる。

第３図においては、カードおよびホストのピンが比較されて整合状態を見出した後（ステップ110 ）、整合するかどうかを判定する（第３図、ステップ120 ）ため、カード・シード10は一般にホストまたはＡＣＭに格納されたカード・シードのライブラリに対して比較される。もしホストまたはＡＣＭ50に挿入されたカード・シード10がホストのライブラリに格納されたシードの１つと一致しなければ、接近または許可は拒絶される（第３図、ステップ120 ）。

最初の説明のため、第１図および第１Ａ図に関連する以下の論議では、本発明の一実施態様により１つの結果的なコード70がホストまたはＡＣＭ50により生成されるものとする。結果のコード40および70を生成するクロック機構、および望ましくは１つのコード70とは対照的にホストまたはＡＣＭが一連の結果の予測不能コードを生じるこの最も望ましい本発明の実施態様については、第４図乃至第９図に関して以下に記述する。

シード10および（または）ピン45を静的変数として使用することに加えて、ユーザに対して最終的に接近または許可90を与える予測不能コード40、70を計算するため、第２の変数である動的変数30、60（第１図、第１Ａ図）を使用するように予め定めたアルゴリズムが構成されている。動的変数は、カード・シード10および（または）ピン45がカード・コンピュータ20またはホストまたはＡＣＭ50のいずれか一方のアルゴリズムに入力される時間間隔で定義され決定されるコード、典型的には１つの番号を含む。動的変数は、静的変数が予め定めたアルゴリズムに入力される日付および時分により定義されることが最も望ましい。このように定義された動的変数は１分毎に変化すると考えることができる。この動的変数は、あるいはまた、どの時間間隔、例えば２分、５分、１時間等に従って定義することもできる。あるいは、このように定義された動的変数は、１分、２分、５分、１時間毎に、または他の予め定めた時間間隔の経過と共に変化する。

第１図においては、このような動的変数を確保する最も望ましい手段は電子的なディジタル・クロックの如き時計装置により、この装置は従来周知の手段によって静的変数10および（または）ピン45の入力（ステップａまたはｃ）に応答して、カード20またはホストまたはＡＣＭ50の予め定めたアルゴリズムに対して日付または特定の時間間隔（例えば、１分、２分、５分等）を自動的に入力する（ステップａ１ またはｃ１ ）。このように時計装置によって生じた日付および時間はそれ自体、動的変数の第１の予め定めたアルゴリズムに対する入力に先立って、別の予め定めたアルゴリズムに従って独立的に操作することができる。予

め定めたアルゴリズムに対して入力される動的変数30または60が予め定めた持続期間の連続的な時間間隔の経過と共に絶対値において常に変化するという事実は、予め定めたアルゴリズムに従って生じたカード・コード40またはホストまたはＡＣＭ70もまた連続する時間間隔と共に常に変化しており、またこれにより全く予測できないことを意味する。

上記のように生成される予測不能コード40、70（第１図）は、（これに対して入力される静的変数10および（または）動的変数30と共に）揮発性の電子的な動的メモリーにおける計算機20（および（または）ホストまたはＡＣＭ50）に格納されることが望ましく、前記メモリーは前記電子メモリーが何等かの方法で侵入、割込みまたは違反される時、アルゴリズム、カード・シード10および動的変数30（または60）を破壊する動作装置と共に包含される。このように前記揮発性の動的メモリーに格納された予め定めたアルゴリズムは犯罪人によって発見され得ないが、これは予め定めたアルゴリズムを含むメモリー全体がメモリーの侵入と同時に破壊されるためである。

従って、本発明の望ましい実施態様においては、カード・シード10は、このような揮発性の動的メモリーに格納され、従来周知の方法でステップａ（第１図）で通常の時間間隔で第１のコンピュータ20のアルゴリズムに対して自動的に入力される。カード・シード10のこのような自動的な入力は、このように第１のコンピュータ20の予め定めたアルゴリズムに対して第１の動的変数30の自動的な定義および入力に関して作用し得、通常の時間間隔における第１の予測不能コードまたは結果のコード40の完全に自動的な生成を行なう。

本発明は、最も望ましくは、認められた人員にカード・コンピュータ20のみを提供するもコンピュータ20に含まれる予め定めたアルゴリズムの知識は提供しない。従って、認められた人員は、このような人員にとって未知であるアルゴリズムを実施することができるコンピュータ20が提供される。

認められたユーザに対して提供あれる予め定めたアルゴリズムがメモリーの侵入と同時にアルゴリズムを破壊する動作手段と共に包含された揮発性の動的メモリーに格納される本発明の最も望ましい実施態様においては、不当な許可または接近を獲得する唯一の手段は元のコンピュータ20、および固定コード／カード・シード10の知識（および、もし本発明と関連して使用されるならば、カードのピン45の知識）を不正に所持することである。

あるいはまた、このアルゴリズムは、１つ以上の固定コードおよび（または）１つ以上の動的変数を操作するように構成することもできる。各固定コードおよび動的変数を入力するいくつかの手段は、ユーザに対して与えられる計算機20およびホストまたはＡＣＭ50に含めることができる（第３図）。各動的変数は、１つ以上の固定コード／カード・シードがアルゴリズムに対して入力される時間間隔により定義されることが望ましい。

従って、予め定めたアルゴリズムは種々のアルゴリズムのどれかを含み得ることが判る。本発明における使用に適するアルゴリズムの唯一の特定の要件は、このようなアルゴリズムが２つの種類の変数、即ち上記の如き静的変数（固定コード）と動的変数に基いて予測不能コードを生じることである。予め定めたアルゴリズムｆ（ｘ，ｙ）により最終的に生じる予測不能コードＣは、下記の如く数式に表わすことができる。即ち、

ｆ（ｘ，ｙ）＝Ｃ

但し、ｘは静的変数／固定コード、ｙは動的変数である。いくつかの（ｎ個）の静的変数（x_1，x_2，．．，x_n）およびいくつかの（ｎ個）の動的変数（y_1，y_2，．．，y_n）が予測不能コードの生成において使用されることが意図される場合には、このように生成された予測不能コードは

ｆ（x_1，x_2，．．，x_n，y_1，y_2，．．，y_n）＝Ｃ

として表わすことができる。

従って、アルゴリズムが不正なユーザにより発見され得る時、アルゴリズムの特定の形態は単に本発明の一部として特定の意義を有するに過ぎな

い。アルゴリズムが包含されたメモリーの意図的な侵入と同時にアルゴリズムを破壊する揮発性の電子的な動的メモリーにおいてこれが格納される故にアルゴリズムが完全に発見され得ない本発明の最も望ましい実施態様においては、特定の形態のアルゴリズムは単に本発明の偶発的な一部を構成する過ぎない。しかし、固定コードおよび動的変数の操作のためあるアルゴリズムを使用するという単なる事実は、このようなアルゴリズムが最終的に意義のある予測不能コードを生成する限り本発明の必然的な部分を構成する。

用語「固定コード」または「カード・シード」または「シード」を本文において用いたが、このような用語はその意味の内に、それ自体が数学的または第2の予測不能コード40（第3図）の生成前またはその間ある非動的な方法で操作あるいは変更される番号、コード等を含む。例えば、第1のコンピュータ20または第2のコンピュータ50は、変数として固定コードまたはシードを用い、予測不能コードを生じる秘密のアルゴリズムにおける固定コードまたはシード10として最終的に入力される新たな固定コードまたはシードを生じる静的プログラム／アルゴリズムを設けることができる。例えば、保全性を増加する目的のため、固定コードまたはシード10は最初に予測不能コードの生成のため用いられた固定コードまたはシード10として使用した別の番号およびその結果に加えることができる。このため、用語固定コードまたはシードとは、その意味に、固定コードまたはシードについて行なわれた非動的操作の結果を含む。従って、どのアルゴリズム即ち演算も別の固定コードまたはシードの生成のため固定コード10について行なうことができ、アルゴリズムまたは演算は最も望ましくは静的アルゴリズム即ち演算かなり、即ち静的結果を生じるように動的変数は用いないことが判るであろう。

第1図においては、第1の予測不能コード40が上記の如く生成された後、このような最初の予測不能コード40が「2番目の」予測不能コード70と比較され、このコードもまた最初の予測不能コード40の生成のため用いられた同じ予め定めたアルゴリズムを含むホストまたはＡＣＭ50に対して固定コード／カード・シード10（および、使用する場合はピン45）を入力する（ステップｃ）ことによりユーザによって生成される。

第1Ａ図（ホストまたはＡＣＭ50が予め定めたアルゴリズムおよび予測不能コードを比較して突合せを行なう機構を含むことを仮定する構成図）においては、許可または接近90を得るため、固定された秘密コード10がホストまたはＡＣＭ50に入力された略々直後に、最初の予測不能コード40がホストまたはＡＣＭ50に対して入力される（ステップe_2）（即ち、ステップe_2は、ステップｅの略々直後に実施される）。もしステップｅおよびe_2がステップａおよびa_1が実施されたと同じ間隔（即ち、コード40が基準とする同じ時間間隔）内で実施されなければ、ホストまたはＡＣＭは、ホストまたはＡＣＭ50の予め定めたアルゴリズムが最初の予測不能コード40と整合する2番目の予測不能コードを生じることを許容する2番目動的変数60を生じることはない。

ステップｅおよびe_2（第1Ａ図）を同じ時分または他の接近された時間間隔（セル）内で実施する必要は、本発明のほとんどの望ましい実施態様においては取除かれる。第3図および第4図においては、カード20は、コード40がカード・クロックにより定義される如く生成された時間セルに基いて結果のコード40を生じる。カード・クロックおよびホストまたはＡＣＭのクロック125が相互および実時間と同期されることを説明のため仮定し、またユーザが適正なカード・シード10および結果のコード40をカード20により生成された結果のコード40と同じ時間セル内にホストまたはＡＣＭ50に対して入れるものとすれば、ホスト50は一連の結果のコード即ち「窓」（第1図の1つの予測不能コード70とは対照的に）を生じるプログラムが与えられることが望ましい。［本文において用いられように、用語「セル」とは、文脈に従って、結果のコードの生成が結果のコード自体に基く予め定めた期間の時間間隔を意味するも

のとする。］「窓」を構成する種々の2番目の予測不能コードは、ユーザがシード10、コード40およびピン45を第3図のホスト・クロック125および第4図に示される如き1つ以上の境界の時間セル例えば－2、－1、および＋1、＋2により定義される如くホストまたはＡＣＭ50に対して適正にエントリする時間セルに基いてホストまたはＡＣＭ50によって計算される。ホストまたはＡＣＭ50のプログラムはこの時、カードの結果のコード40を第4図に示されるホスト・セルの窓として計算される全ての個々の結果コードと比較して、ホスト・セルのどれかとカード・コード40との間に整合状態が存在するかどうかを判定する。上記の事例においては、カード・コード40は無論第4図の零のセルに基くホスト・コードと整合状態となる（第3図、ステップ172）が、これはユーザがカード・コード40が生成された同じ時間セル内にシード10、ピン45およびコード40を入れるためである。

［本文に用いられる如く、ホストまたはＡＣＭ50に対する「入力」または「入力すること」または「エントリ」とは、ホストまたはＡＣＭ50に対する適正なカード・シード10、カードの結果コード40およびカードのピン45の入力、およびカード・シード10（第3図、ステップ120）およびカードのピン45（同、ステップ110）のホストまたはＡＣＭ50における恒久メモリーに格納されるホスト・シードおよびホスト・ピンに対する確実な整合を意味する。］

しかし、第4図に関して先に述べた事例においてユーザがカード・コード40およびカード・シード10（およびピン45）をカードがコード40を生成した1分後に入力（第3図）したものとすれば、ホストまたはＡＣＭ50は第5図に示される如き異なる窓を生成したことになり、即ちホストがあたかも＋1のセル・コードがセルの窓の零のセルであり（第5図において括弧内に示す如く）かつ更に予め定めた数の境界の時間セルのコードを生成する（例えば、第5図に示されるように実時間－1、0および＋2、＋3）如く、＋1のセル・コードと対応する中心のセルを生成したことになる（実時間に基いて）。このように、ユーザはカード・シード10およびカードの結果コード40を1分後ホストまたはＡＣＭ50に対して入力するが、ホスト・コンピュータ50は、整合するセル・コード、中心のセル即ち第5図において括弧内に示される如き＋1の中心セル・コードの「境をなす」実時間零のセル・コードを依然として生成する。

ホストまたはＡＣＭ50（第3図乃至第5図）に第1図の単一の2番目コード70とは対照的に一連の即ち2番目の予測不能コードの窓を生成する機構を提供することにより、適正なシード10とピン45とカードのコード40をホストまたはＡＣＭ50に対して入力しかつ依然として整合するホストの結果コードを生じるある選択された量の時間の裕度（コード40が基く時間間隔の長さを越える）をカード・カード・ユーザに許容する。

上記の事例は、カード・クロックおよびホスト・クロック125（第3図）が共に実時間と同期することを仮定していた。コード・クロックおよびホスト・クロックが常に同期した状態を維持するものとすれば、ホストまたはＡＣＭ50に窓の中心のセルの「前方にある」ある予め定めた数の間のセル、例えば第5図における（－2）、（－1）、（0）のセルを生成する機構を提供することのみが必要となる。カード・クロックおよびホスト・クロックが常に相互に同期した状態に維持される如き用途においては、ホストまたはＡＣＭのクロック125が1つの中心のセルのコードおよび1つの－1のホストの窓のセル・コードを生成するように2つの動的時変数しか規定しないことが望ましい。この実施例では、ユーザがシード10、ピン45およびコード40に対して1つのセル・コードを入力するが機密保護の強化のため後で唯1つのセル・コードを入力することを許容する。

しかし、カード・クロックおよびホスト・クロック125が実時間との同期状態から外れ得る更に典型的な場合、例えばカード・クロックがホス

ト・クロックに比して進む場合においては、整合するホストの結果のコードを生じるためホストの窓の中心セルに「疾く」セルの生成が必要となる。

第3図および第6図においては、本発明は最も望ましくは、カード・クロックおよびホスト・クロックの如き独立的なクロックが更に典型的に実時間および（または）相互に進むかあるいは送れる場合においてこれらのクロックを同期させるための機構を提供する。

下記の事例は、説明の目的のため、全てのセル・コードの等しい時間長さが持続期間1分であるものとする。このカード・クロックが1分遅れ、ホストのクロック125（第3図）が実時間に対して適正であるものとすれば、カードは－1分の実時間（ホストのクロック125に対して）に基いて結果のコード40を生成することになり、またもしユーザがカードの結果コード40（および適正なシード10とピン45）をコード40が生成されると同じ時分内にホストまたはＡＣＭ50に対して入力するならば、ホストまたはＡＣＭ50は第6図に示した一連のセルに従って結果のコードの窓を生じることになる（予め定めた数の間のセルが直前の2つのセルと直後の2つのセルとして選択されるものとすれば）。整合する結果のコード、即ちカードの－1のセル・コードおよびホストの－1のセル・コードがこのように生成されることになる。

カード・クロックがこの事例において1分遅れていたが、ホスト・コンピュータはカードのユーザが次に適正なカード・シード10およびカードのピン45（およびコード40）をホストまたはＡＣＭ50に対して入力する時、カード・クロックの時間でホストのクロックの時間を自動的に調整（即ち、同期）することになるプログラム機構が設けられる。このホストは、ホストの恒久メモリーに整合するセル時間の差を格納する（第3図、ステップ190）ことによりこのような同期を達成する。例えば、今述べた許りの事例においては、最後の整合取引き（第3図、ステップ 180）は第6図における括弧に示したようにホストの「窓」の－1のセルに該当する。このようなセルの時間差は、本文においては、ホストの恒久メモリーに格納される「時間のずれ」と呼ばれる（第3図、ステップ 190）。この時間のずれは、これから整合する2番目の予測不能コードが生成された中心のセルと間のセルとの間の時間差である。

カードのユーザのホスト50に対する次のエントリと同時に（カード・クロックが最後のエントリ以後全く遅れていなかったものとし、またホストのクロックが実時間と同期した状態を維持しかつカードが結果のコード40を生成すると同じ時分内にユーザが次にエントリするものとすれば）、ホスト・コンピュータ50は自動的に格納された時間のずれを一時的に格納されたホスト・クロック時間に対して（第3図、ステップ 130）代数的に加算し（同、ステップ 140）、また第7図に示される一連の相対的な実時間のホストのセル・コードを生成することになるが、これにおいては実時間で1分遅れたカードのコード・セルがこの時ホストの窓において零のセルとして処理され（第7図の括弧内に示される如く）、即ちホストのセルの窓の中心のセルが第3図の1分格納された時間のずれ135の控除を経てこれから1分を差引くよう調整される。第7図に示されるように、ホストの窓の間のセルは同様に1分格納された時間のずれだけ調整される。更に、ホスト50に対するユーザの全ての将来のエントリにおいては、一時的に格納されたエントリの時間および日付（第3図、ステップ 130）は恒久的に記録された1分間格納される時間のずれだけ調整されることになる。

カードおよびホストのクロックが実時間と同期されることを仮定し、またユーザがホストの1分後にエントリした第5図に関して上に述べた事例に関して、例えホストのクロックが実時間と同期されても、ホストはそれにも拘らず格納されかつユーザによる将来の取引きにおいて一時的に格納されたエントリの時間（第3図、ステップ 130）を調整する際使用されるべき（第3図、ステップ190）時間のずれを計算することになる（同、ス

テップ 180）が、これは第5図の括弧内に示される如きホストの窓の整合するセルが窓の中心のセル・コードではなく（即ち、実時間＋1のセル・コードではなく）、むしろ間の実時間のセル・コード即ち間の実時間の等のセル・コードであったためである。

従って、簡単にいえば、格納された時間のずれは計算され（第3図、ステップ 180）、あるエントリにおいて（第3図、ステップ 130）ホストの窓の「間の」セル・コードが（中心のセル・コードとは対照的に）入力カードの結果のコード40との整合状態を生じる時は常に、全ての将来のエントリにおいてホストに対するエントリの時間を調整する（第3図、ステップ 140）際に使用するため格納される（第3図、ステップ 180）。

ある取引きの間計算される（第3図、ステップ180）時間のずれを格納する際（ステップ190）、この時計算された時間のずれは、前のエントリおよび接近の許可の結果として前に計算されて格納されたどの時間のずれに対して代数的に加えられ即ち加算される（ステップ 173）。

クロック機構は、一旦進みまたは遅れ始めると、本発明のシステムのあらゆる将来の使用において進みあるいは遅れ続けることになるため、ホストまたはＡＣＭ50は前の取引きから記録され恒久的に格納される格納済みの時間のずれに対しシステムの連続的な使用中記録された全ての時間のずれを加除する（第3図、ステップ 180）ことになる。更に望ましくは、新たに計算された時間のずれは、接近または許可が既に許与されずまた許容される（ステップ 173）までは、ホストまたはＡＣＭのメモリー200 には恒久的に格納されない（ステップ 190）。

第4図乃至第7図において述べまた示すように、ユーザがカード・シード10、パルス45およびカードの結果コード40のホストまたはＡＣＭへの入力において変更することを許される「窓」として、ホストまたはＡＣＭは中心のセル・コード間4つのセル・コード（即ち、中心のセルの直前の2つのセルと直後の2つのセル）を計算するように典型的にプログラムされている。このような間のセルは1分の間隔と対応するコードに対応する如く述べた。間のセルの数および時刻に相当する長さが必要に応じて増減することができることが判る。

カード・クロックおよびホストまたはＡＣＭのクロックが実時間に対して進みあるいは遅れる絶対的な程度は一般に時間の進行と共に増加する。例えば、もしカード・クロックが1月に30秒だけ遅れ、ホストのクロックが1月に30秒だけ進むならば、この2つのクロックは、1月後に同期状態からずれる1分、2月後に同期状態からずれる2分、3月後に同期状態からずれる3分、、、等に相当する時間だけずれを生じることになる。もし許可されたカードのユーザが毎月このカードを使用するならば、第4図乃至第7図に関して先に述べた自動同期装置は、実時間に対するこのような同期の欠如を補うように使用の都度ホストまたはＡＣＭの時間の窓を調整することになる。しかし、もしカードのユーザが実際にこのカードを例えば6箇月間使用しなければ、カードのクロックおよびホストのクロックは6分間同期状態からずれることになり、また例えユーザがピン45、カード・シード10およびカードの結果コード40をピン45、シード10およびコード40がカードにより生成されると同じ時分内にホストまたはＡＣＭに対して入力する（第3図）ことにより正しく本システムを使用しても、ユーザは間のセル時間の「窓」が中心のホスト・セルに対して直前の2つの1分セルおよび直後の2つの1分セルとして選択される典型的な場合において接近または許可を得る（即ち、ホストまたはＡＣＭに整合する結果のコードを生じさせる）ことができないことになる。第8図は、今述べたこのような事例の場合を示し、これにおいては6箇月間使用しなかった後、カード・クロックは実時間で－3分に基く結果のコード40を生じ（第3図）、また6箇月の不使用の後ホストのクロックは実時間に対して＋1、＋2、＋3、＋4および＋5分に対応するセル・コードからなる典型的に選定された5つの

セルの窓の生成をもたらすことが判る。従って、選択された窓が4つの間のセルからなるこの典型的な場合においては、6箇月の不使用の後は如何なる状況下でも整合する2番目の予測不能コードが生成されないことになる。

本発明は、最も望ましくは、間のセルのホストの窓がカードの不使用の期間の長さと共に変化する量だけ予め選定された窓よりも広く開かれる機構を提供する。このような窓の開放は、比較および突合せの最も近い日付を格納し、このような日付と第2のコンピュータに対するエントリの現在の日付との間の差を判定し、これら日付間の差に従って予め定めたものと同数の別の境界の時間セルを計算することにより達成される。

典型的には、この窓は不使用の月当り2つの1分の境界の時間セル（例えば、予め選定された窓の直前の1つのセルおよび直後の1つのセル）だけ開かれるが、窓が開かれるセルの数および各セルの時間相当長さは他の所要の数および長さを構成するように予め定めることができる。

に、整合するホストのセル・コードはホストの窓の1つの間のセル・コードであって中心のホスト・セル（即ち、零のセル）ではないため、新たな格納された－6分の時間のずれが計算され（即ち、恒久的に格納された時間のずれに加算され）（第3図、ステップ180）、格納され（ステップ190）、その後ホストのクロックは、その時の取引きにおいて使用された特定のカード・シード10およびピン45を有するカードのユーザがこのカードを使用して将来の取引きにおける接近を得る毎に、ホストの窓の零のセル（およびこれに伴なう境界の時間セル）を調整することになる。

最後に、本発明は更に、ホストまたはＡＣＭ50およびそのクロック125（第3図）がカードの使用間に停止する不慮の事故に対応するフェールセーフ窓開放機構を含む。このような停止の場合には、ホストまたはＡＣＭのクロック125は一般にリセットして再び同期されねばならず、またこのような再セッティングの過程においては、再同期操作において誤差が生じ得る。カードのユーザ

カードのクロックおよびホストのクロック125（第3図）が月当り30秒だけ相対的な進みおよび遅れを生じかつユーザが6箇月間カードを使用しなかった上記の事例を想定すると、ホストまたはＡＣＭは、最後の選択の恒久的に格納された（ステップ175）日付に対してその時のエントリの一時的に格納された（ステップ130）日付を比較し（ステップ150）、最後の接近の日付とその時のエントリの日付との間の月数×を計算する（ステップ180）。本例においては、6箇月の不使用が計算され（ステップ180）、また窓は18分の完全な窓を与えるように第9図に示すように予め選定された4つのセルの窓のいずれかの側に更に6つの1分の境界の時間セルだけ開かれる。相対的な実時間における－3分に基くカードの結果コード40は、このように第9図に示されるように、－6のホストの境界の時間セル・コード（実時間における－3）に対して整合し（第3Ａ図、ステップ172）、最後に接近または許可が与えられる。第4図乃至第7図に関して先に述べたように

がこのようなホスト・クロック125の再セッティングにおける誤差の場合に順当な接近を得ることができることを保証するため、ホストまたはＡＣＭ50はこのような再セッティングを検知してホストまたはＡＣＭ50の再セッティング毎に予め定めた窓開放番号を格納するための機構が設けられることが望ましい。このような窓開放番号は、典型的には6つの別の1分の境界の時間セル（例えば、その時の窓の直前の3つの別のセルおよび直後の3つの別のセル）として選定されるが、他の選定された長さのこれ以上もしくは以下の数のセルとして選定することもできる。

前記の再セッティング窓開放番号は典型的には不使用の結果（第3図、ステップ160）に加算され（同、ステップ165）、この窓を構成する更に別の総数が計算され（ステップ170）、即ち、（ａ）入力に際するユーザの遅れおよび（または）カードおよびホストのクロックの非同期を許容する予め選定された窓、（ｂ）長期の不使用にわたるカードおよびホストのクロックの非同期を

許容する不使用の窓、および（ｃ）再セッティングの窓開放番号を含む中心のセルの周囲の全ての間のセルが計算される。

第９図に関して本文に述べた事例を仮定して、もしホストまたはＡＣＭが不使用の６箇月の期間内に停止したならば、第９図に示される如きホストの窓は、－11、－10、－９および＋９、＋10、＋11のホストの窓のセルもまた計算され（第３図、ステップ170）また第３図のステップ172においてカードの結果コード40との比較および潜在的な整合のため使用可能にされるように、更に別の６つの間のセルによって更に開かれることになる。新たな時間のずれが計算され格納される（第３図、ステップ180、190）第５図乃至第９図に関して述べるように、不使用および（または）予め選定された窓により生じる窓の間のセルにおいて見出される整合状態の結果として、もし停止の結果生じた間のセルにおいて整合状態が見出されるならば、新たな時間のずれが同様に計算されて格納される（ステップ180、190）ことになる。

不使用の窓開放番号とは異なり、再セットされた窓開放番号は典型的には、一旦ホストのクロック125が再びセットされると、ユーザにより次に試みられるエントリと同時に窓を開放するため恒久的メモリー200において選択された窓開放番号が使用できるように、ホストまたはＡＣＭ50の恒久的メモリー200において格納される（第３図）。再びセットされた窓開放番号は確立され恒久的メモリー200に格納されるが、ホストのクロック125が適正にリセットされた連続的に試みられたエントリと同時に種々のカード・ユーザによって確立された後、あるいは再セッティングの結果として生じ得る誤差の訂正のためホストのクロック125が他の方法で実時間と再び同期された後、このような再びセットされた窓開放番号は最後には閉じられるかあるいは保全の強化のため取払われることが望ましい。従って、再びセットされた窓開放番号の使用は一時的なものであることが望ましい。

本発明の実際の応用においては、多数のユーザに対して多数のカードが発行され、また各カードはそれ自体のカード・クロックを含む。色々なカードの統計的に意義のあるサンプルの個々のクロックにより保持される時間の平均が実時間の正確なあるいは非常に近似した正確な表示を生じることになることを認識して、本発明は、クロック125がリセットされた後にホストのクロック125により保持された時間をある選択された数の異なるカードまたはカード・ユーザの（ホストのクロック125の再セッティング後の）エントリ回数の平均値に対して恒久的に調整する（第３図）ための機構を含むことが最も望ましい。例えば、ホストのクロック125がリセットされたものとすれば、次の５人（もしくは他の数）の個々のカード・ユーザの次のエントリ時点が平均化され、ホストのクロック125はこのような平均時間に対して恒久的に調整あるいは再び同期され、その後リセットされた窓開放番号は恒久的なホストのメモリー200から除去される。カード・クロックの平均時間に対するホストのクロック125の再調整または再同期は、各カード20に固有の時間のずれに対して代数的に加算される別のマスターの時間のずれを計算することにより、ホスト50によって実施されるのが典型的である。このようなマスター時間のずれの計算は、リセットされた窓の開放その他の結果として選択された数の個々のカード20が接近を得ることができたものとする。（ホストのクロック125がリセットされた後）ホスト50に入る選択された数のカードについて計算された時間のずれの平均は、マスター時間のずれとして（即ち、ホストのクロック125の再同期として）格納されることが望ましく、次にこのリセット窓開放番号はカード・ユーザによる全ての将来のエントリについて除去され、マスター時間のずれはその後の全てのカードのエントリに関する取引きにおけるカード・クロック125を調整するため使用される（各カードに固有の恒久的に格納された時間のずれに加えて）。

実際問題として、カード・ユーザが使用しない

期間の長さまたはホストまたはクロック125 の再セッティングの結果としてＡＣＭ50がリセットされる回数の如何に拘らず、窓が開放される間のコストの総数には一般にある制約が課される。機密保持の理由から、このような制限は一般に第３図のステップ170 に示される如き10の１分の間のセルとして選択され、窓を構成するコード数は、（ａ）４つの間のセル・コード、即ち望ましい選択された窓、プラス月数または他の選択された不使用期間ｘ、プラス停止した窓開放番号ｙ、または（ｂ）別のセル・コードの最大数である10の小さな方である。このような最大の窓は、無論、所要の機密保持の程度に応じて10以上もしくは10以下として選択することができる。

第３図は必ずしもシーケンスのみではないが操作の望ましいシーケンスを示すことが判る。例えば、ステップ110 および100 は、リセットされた窓開放番号を自動的に入力するステップと交換することができるが、ステップ167 はステップ140 ～160 のいずれよりも先行し得る。

クレジット・カード・コンピュータ20（第２図）は、その表面に印刷されたカード・シード固定コード10の指標を保有し、ディジタル・クロック装置、動作装置、マイクロプロセッサ、および予め定めた秘密のアルゴリズム、必要に応じて動的変数および必要ならばじカード・シード10およびピン45を生成するプログラムを格納するため充分なメモリーを含む。

物理的な施設に対する接近を許容することが目標である本発明の一実施態様においては、ＡＣＭ50は保護体制に置かれた建物または他の施設に至る中央の接近場所に置かれた保全監視員により保持することができるように携帯可能な装置を構成することができる。このようにこのようなＡＣＭを所持する保全監視員は、許可された人員のカード20上に現われるカード・シード10および予測不能コード40（第２図）を読み、これらのコード10、40を（さもなければカードの所持人により監視員に提示されたピン45に加えて）携帯可能なＡＣＭ50に対して入力して、カードの所持人が秘密の予め定めたアルゴリズムを確立する所轄部署により発行されたカード20の正当に保持するものであるかどうかを判定する。

第１図、第１Ａ図および第３図のホストまたはＡＣＭ50は、１つ以上のこのような機能はホストまたはＡＣＭ50とは別個でこれと通信しあるいはこれと結合された装置によって実施することもできるが、一般に１つ以上のプログラムと第３図に示された全てのステップを実施するに充分なメモリーを含む。

時間のずれの計算、格納および検索に関して、ホストまたはＡＣＭ50には、各カード・シード10および（または）ピン45に固有ものでありかつホストまたはＡＣＭ50への入力に応じる時間のずを認識し、格納し、検索し、計算する機構が設けられる。

第２図は、最初の予測不能コードまたはカードの結果コード40を生成するため許されたユーザに対して与えられる計算機20の最も望ましい形態を示している。第２図に示されるように、この計算機20は従来のクレジット・カードと略々同じサイズであり、コード40をユーザに対して表示するための従来周知の液晶ディスプレイ44を含む。この

本文に述べように、予め定めたアルゴリズムの秘密の保護は、揮発性の動的メモリーおよび揮発性の動的動作装置と一緒に密閉されることにより許可された人員に対して与えられた計算機において行なわれることが望ましい。ＡＣＭに与えられたアルゴリズムに関しては、同様な方法あるいは他の周知の方法、例えばＡＣＭを物理的に保護するかあるいは直接の接近を得るためには別の接近／ユーザ・コードを必要とすること等により維持することができる。全てのプログラム、データおよび操作の結果がこのような揮発性動的メモリーに格納される場合は、これらも同様に侵入から保護される。

本発明はカード20に保持された操作の結果40（第２図）のホストまたはＡＣＭ50もしくは他の電子的装置に対するある形態の通信に関するものであるが、コンピュータ20とホスト50との間の対

話は本発明においては必要でないかあるいは対象とならない。従って、第1のコンピュータ20が計算した後で、第1の予測不能コード40およびコード40がホスト50に対して入力され、許可または接近を得るために他の情報はホスト50もしくは他の装置から第1のコンピュータ20に対して逆に通信する必要はない。

最後に、固定コードまたはシード10および（または）ピン45（第3図）を使用して、カード20に対応するコンピュータ端末または設備の他の装置または装置を識別することができる。例えば、端末または宇宙衛星または他の装置には、カードのコンピュータ20が上記の如く識別されると同じ方法でこのような端末、衛星等を識別するため、コードまたはシード10および（または）ピン45が割当てられたコンピュータ20の提供が可能である（また、無論、秘密の予め定めたアルゴリズムおよびクロックおよびコード40を計算してコスト10、ピン45および結果のコード40をホストまたはACM50に対して入力するための周知の電子的機構が設けられる）。

当業者には、頭書の特許請求の範囲によってのみ限定される本発明の開示の主旨および範囲に従って他の実施態様、改善、細部変更および使用が可能であることが明らかであろう。

4　図面の簡単な説明

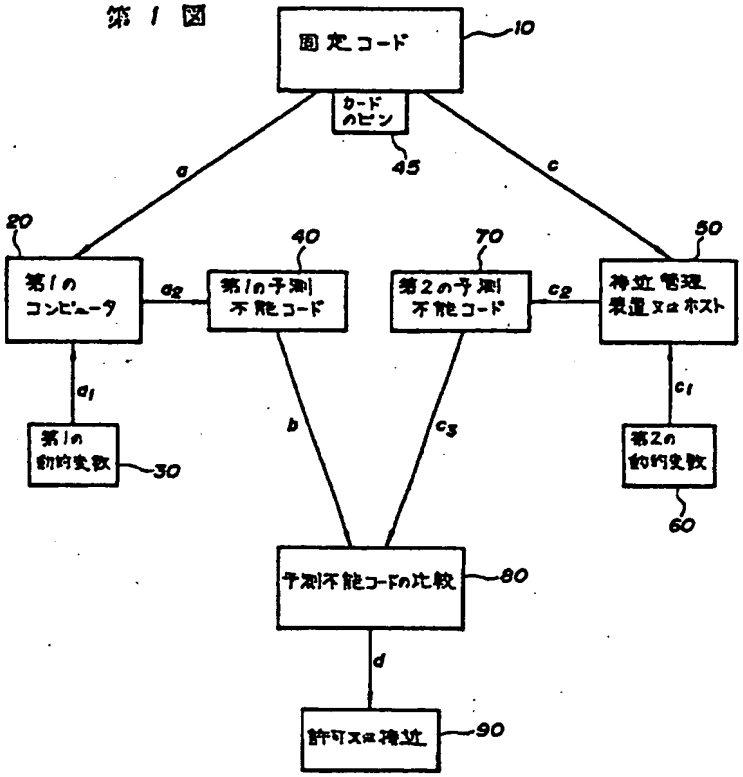
第1図は予測できないコードを生成して比較するための本発明による基本的な装置および方法を示すブロック図、第1A図は予測できないコードを比較する装置が予測できないコードを生成する計算機に含まれる予測できないコードの生成および比較のための望ましい装置および方法を示すブロック図、第2図は本発明による許可または接近を得る際使用される第1の予測できないコードを計算するクレジット・カード寸法の計算機を示す斜視図、第3図は本発明による装置および（または）方法により実施される最も望ましい一連のステップを示すフローチャート、および第4図乃至第9図は本文に述べる事例による個々のコンピュータにより結果として個々に生じる一連のコード・セルを示し、各図に関して記述する対応した例示的な条件により結果として得るコードを生じる個々のコンピュータにおける個々のクロック機構により保持される如き時間に基いて結果として生じるコード間の実時間との関係を示す図である。

10…固定コード／カード・シード、20…計算機、30、60、60…動的変数、40、70…予測不能コード、45…ピン、44…液晶ディスプレイ、50…接近監視装置／ホスト、80…予測不能コード比較装置、90…許可／接近、125 …ホスト・クロック、200 …恒久的メモリー。

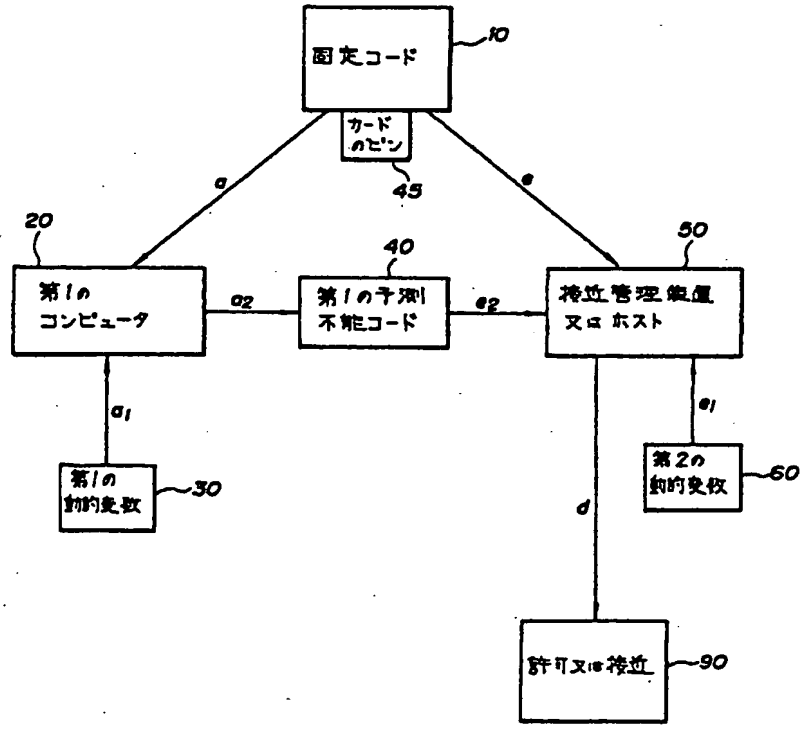
代理人　弁理士　湯浅恭三

図面の簡単

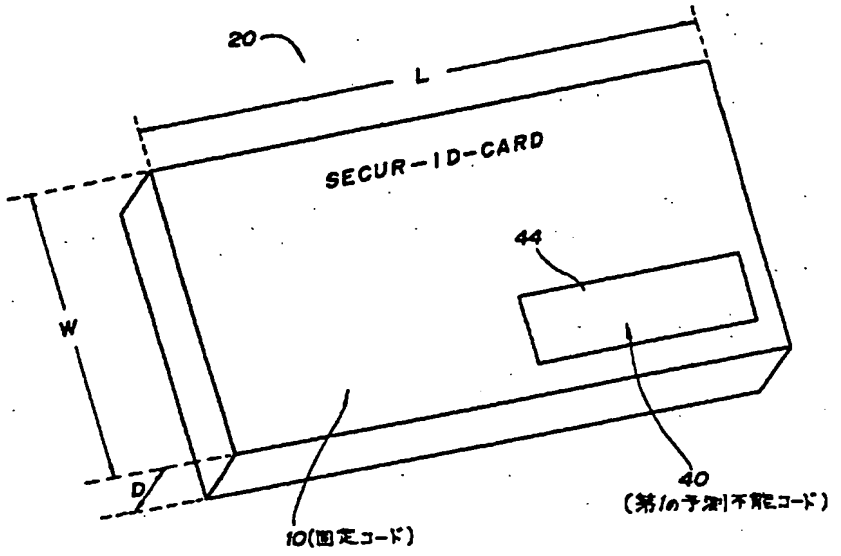
第 1 図



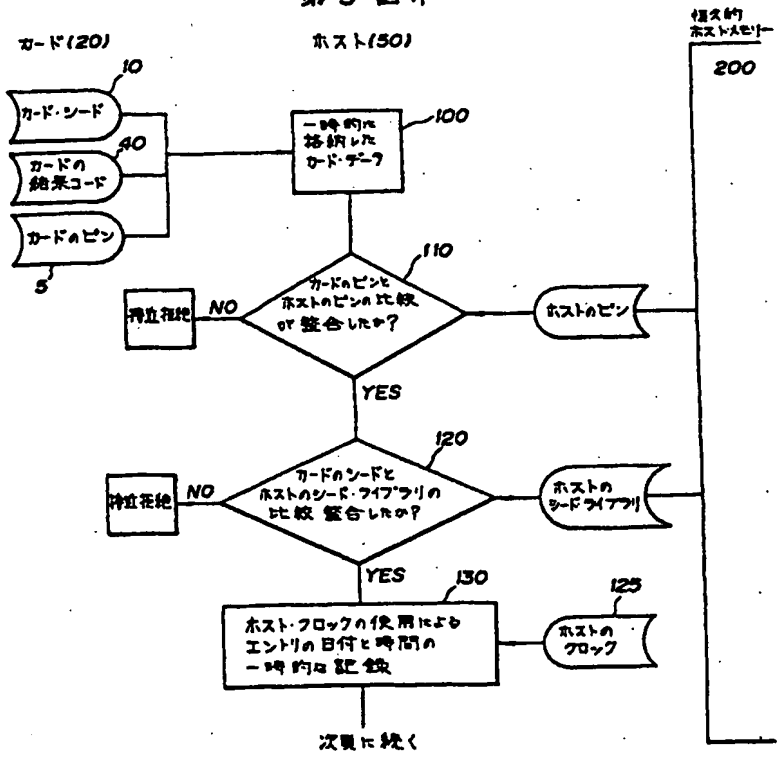
第 1 図 A



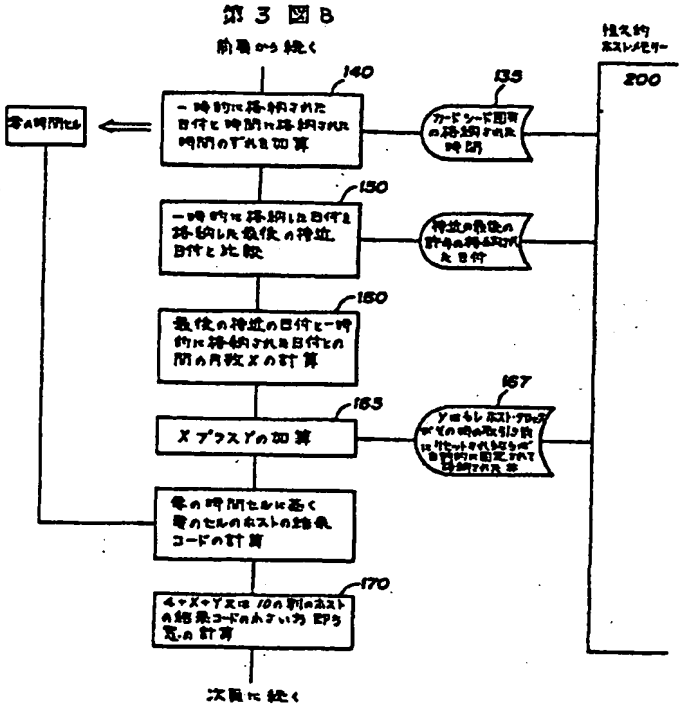
第 2 図


20
L
SECUR-ID-CARD
44
W
D
40
(第1の予測不能コード)
10(固定コード)

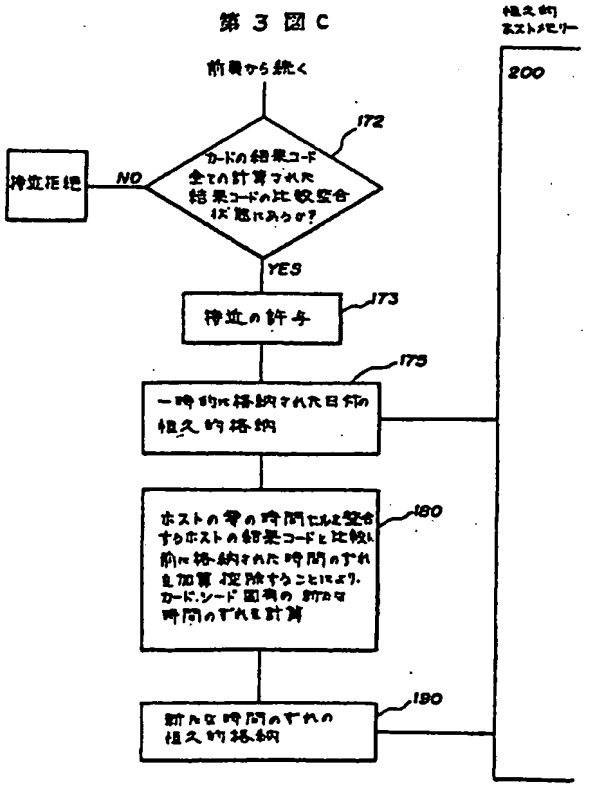
第 3 図 A


カード(20)
ホスト(50)
恒久的ホストメモリー
200
10
カード・シード
40
カードの始発コード
カードのピン
5
一時的に格納したカード・データ
100
110
カードのピンとホストのピンの比較 が整合したか?
NO
排他拒絶
ホストのピン
YES
120
カードのシードとホストのシード・ファイルの比較 整合したか?
NO
排他拒絶
ホストのシードファイル
YES
130
ホスト・クロックの使用によるエントリの日付と時間の一時的な記録
125
ホストのクロック
次頁に続く

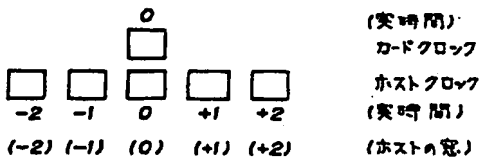
第３図Ｂ



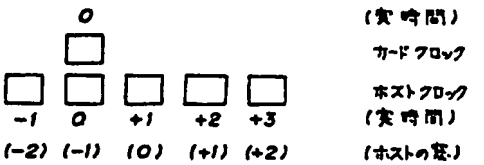
第３図Ｃ



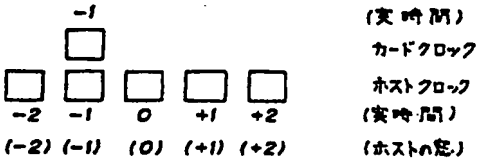
第４図



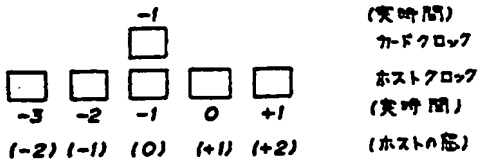
第５図



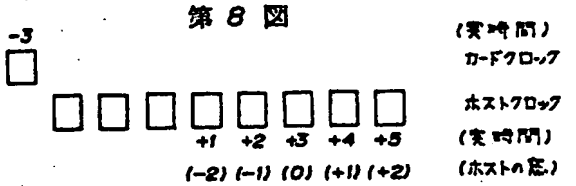
第６図



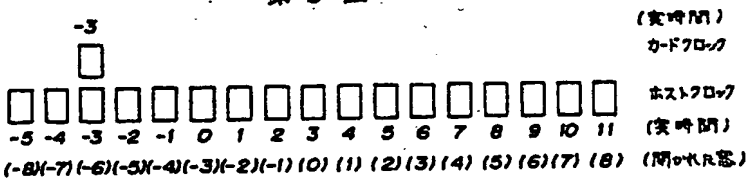
第７図



第８図



第９図



手　続　補　正　書

昭和６２年６月ﾉ7日

特許庁長官　黒　田　明　雄　殿

1．事件の表示

昭和６１年特許願第２８３０４１号

2．発明の名称

別個の時間動作装置を同期させる装置および方法

3．補正をする者

事件との関係　特許出願人

住所

名称　セキュリティ・ダイナミックス・テクノロジーズ・インコーポレーテッド

4．代理人

住所　東京都千代田区大手町二丁目2番1号
新大手町ビル２０６号室
電話(270)－6641～6

氏名 (2770) 弁理士　陽　捨　善　三

5．補正の対象

明細書の〔特許請求の範囲〕、〔発明の詳細な説明〕と〔図面の簡単な説明〕の欄

6．補正の内容

別紙の通り

（別紙）

1．〔特許請求の範囲〕を次の通りに補正します。

「(1) 時間に従って個別のクロック装置により定義される動的変数に基いて個別のコンピュータにより生成される予測不能コードを比較して突合せを行なうシステムにあって、前記動的変数の時間的定義を同期させる装置において、

ある予め定めたアルゴリズムに従って第１の予測不能コードを計算する第１のコンピュータを設け、該アルゴリズムは第１の動的変数および一般的な静的変数に基いて前記第１の予測不能コードを生成し、

前記静的変数が前記アルゴリズムに対し入力される第１の時間間隔に従って前記第１の動的変数を自動的に定義する第１のクロック装置を設け、前記第１の時間間隔は第１の予め定めた持続期間を有し、

前記予め定めたアルゴリズムに従って２つ以上の第２の予測不能コードを計算する第２のコンピュータを設け、該アルゴリズムは２つ以上の第２の

動的変数と一義的な静的変数に基いて前記第２の予測不能コードを生成し、

前記静的変数が前記第２のコンピュータのアルゴリズムに対し入力される第２の時間間隔の２つ以上のセルに従って前記２つ以上の第２の動的変数を自動的に定義する第２のクロック装置を設け、該第２の時間間隔は１つの予め定めた持続期間を有する１つの中心の時間セルと、該中心の時間セルの境界をなす１つ以上の時間セルとからなり、各境界の時間セルはある予め定めた持続期間を有し、

前記第１の予測不能コードを前記第２の予測不能コードと比較して整合状態を判定する装置と、

前記第２の予測不能コードの内の１つに対する前記第１の予測不能コードの比較および突合せと同時に、前記第１のクロック装置と前記第２のクロック装置とを自動的に同期させる装置とを設けることを特徴とするシステム。

（２）前記中心の時間セルが、前記の一義的な静的変数が、第２のコンピュータに対して入力される、前記第２のクロック装置により定義される如き日付と時分とからなることを特徴とする特許請求の範囲第１項のシステム。

（３）前記境界の時間セルが、前記中心の時間セルの直前の日付と時分とからなることを特徴とする特許請求の範囲第２項記載のシステム。

（４）前記同期装置が、

整合する第２の予測不能コードを生成するとができる中心の時間セルと境界の時間セルとの間の時間的差をカウントするカウント装置と、

該カウント装置によりカウントされる連続する時間的差を加算するため前記カウント装置と結合された加算装置と、

該加算装置の出力を格納するため加算装置と結合された格納装置と、

該格納装置に格納された加算された時間だけ中心の時間セルと境界の時間セルとをシフトするため前記格納装置と結合されたシフト装置とを含むことを特徴とする特許請求の範囲第１項記載のシステム。

（５）前記境界の時間セルが、前記中心の時間セルの直前のある選択された数の時間セルと、前記中心の時間セル直後のある選択された数の時間セルとからなることを特徴とする特許請求の範囲第４項記載のシステム。

（６）前記中心の境界の時間セルが持続期間が１分となるように選択されることを特徴とする特許請求の範囲第５項記載のシステム。

（７）前記同期装置が更に、

最も後の比較の日付を格納して前記比較装置による突合せをするため前記比較装置と結合された第２の格納装置と、

格納された前記日付と、前記第２のコンピュータに対するその時のエントリの日付との間の時間的差をカウントするため前記第２の格納装置と結合された第２のカウント装置と、

ある選択された値により前記第２のカウント装置によりカウントされた時間的差を除し、出力を第１の窓開放番号として定義するため前記第２のカウント装置と結合された除算装置と、

前記第１の窓開放番号により定義される如き選択された数の前記境界のセルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第２の予測不能コードを計算するため前記除算装置および前記比較装置と結合された窓開放装置とを含むことを特徴とする特許請求の範囲第５項記載のシステム。

（８）前記同期装置が更に、

前記第２のクロック装置の再セッティングを検出するため第２のクロック装置と結合された検出装置と、

ある選択された第２の窓開放番号として前記第２のクロック装置の検出された再セッティングの発生を定義してこれを格納するため前記検出装置と結合された第３の格納装置と、

前記第２の窓開放番号により定義される如き別の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第２の予測不能コードを計算するため前記第３の格納装置と結合された第２の窓開放番号装置とを含む

ことを特徴とする特許請求の範囲第7項記載のシステム。

(9) 前記第1のコンピュータが、前記アルゴリズムを動作装置と共に包含された揮発性の動的メモリーに格納するマイクロプロセッサを含み、前記動作装置は、割込みされた時、少なくとも前記アルゴリズムおよび静的変数を含む全てのデータを破壊することを特徴とする特許請求の範囲第8項記載のシステム。

(10) 前記第1のコンピュータと前記第1のクロック装置とがクレジット・カードと略々同じサイズのカードに内蔵されることを特徴とする特許請求の範囲第9項記載のシステム。

(11) 前記第2のコンピュータのアルゴリズムが、動作装置と共に包含された揮発性の動的メモリーに格納され、前記動作装置は、割込みされた時、少なくとも前記アルゴリズムおよび前記静的変数を含む全てのデータを破壊することを特徴とする特許請求の範囲第10項記載のシステム。

(12) 動的変数が整合する時コードが整合する、

時間に従って個別のクロック装置により定義される動的変数に基いて別個のコンピュータにより生成される予測不能コードを比較する方法であって、前記動的変数の時間の定義を同期する方法において、

ある静的変数をある予め定めたアルゴリズムを含む第1のコンピュータに対して入力し、

該第1のコンピュータのアルゴリズムを用いて、前記静的変数と、第1のクロック装置に従って前記入力ステップが生じた第1の時間間隔により定義される第1の動的変数とに基いて第1の予測不能コードを計算し、

前記静的変数と前記第1の予測不能コードとを前記予め定めたアルゴリズムを独立的に含む第2のコンピュータに対して入力し、

前記第2のコンピュータのアルゴリズムを用いて、前記静的変数と、前記入力ステップが第2のクロック装置に従って生じた第2の時間間隔の2つ以上のセルにより定義される2つ以上の第2の動的変数とに基いて第2の予測不能コードを独立

的に計算し、前記第2の時間間隔は1つの中心の時間セルと1つ以上の境界の時間セルとからなり、

前記第1の予測不能コードを前記第2の予測不能コードと比較して整合状態を判定し、

前記第2の予測不能コードの内の1つに対する前記第1の予測不能コードの比較および突合せと同時に、前記第1のクロック装置と前記第2のクロック装置を同期させるステップとからなることを特徴とする方法。

(13) 前記同期ステップが、

整合する第2の予測不能コードを生成し得る1つの中心の時間セルと1つの境界の時間セルとの間の時間的差をカウントし、

該カウント・ステップにおいてカウントされた連続する時間的差を加算し、

加算された連続する時間的差を格納し、

加算された前記連続する時間的差だけ前記中心および境界の時間セルをシフトするステップを含むことを特徴とする特許請求の範囲第11項記載の方法。

(14) 前記同期ステップが更に、

整合状態の最も後の比較および判定の日付を格納し、

前記格納された日付とその時の第2のコンピュータへのエントリの日付との間の時間的差をカウントし、

前記日付の差をカウントする前記ステップの間カウントされた差をある選択された値により除して、出力を第1の窓開放番号として定義し、

前記第1の窓開放番号により定義される如き前記選択された数の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第2の予測不能コードを計算するステップを含むことを特徴とする特許請求の範囲第11項記載の方法。

(15) 前記同期ステップが更に、

前記第2のクロック装置の再セッティングを検出し、

前記第2のクロック装置の検出された再セッティングの発生を第2の選択された窓開放番号として

定義して格納し、

前記第2の空開放番号により定義される如き別の境界の時間セルの直前および直後の多数の別の境界の時間セルに基いて、これと同数の別の第2の予測不能コードを計算するステップを含むことを特徴とする特許請求の範囲第11項記載の方法。

(16) 前記中心および境界の時間セルが持続期間において1分となるように選択されることを特徴とする特許請求の範囲第12項記載の方法。

(17) 予測不能コードの電子的な生成および比較を行なう装置において、

ある予め定めたアルゴリズムに従って第1の予測不能コードを計算する第1の装置を設け、該第1の計算装置は、一義的な静的変数を前記予め定めたアルゴリズムに対して入力する第1の装置を含み、

前記第1の入力装置が付勢される時間間隔に従って第1の動的変数を自動的に定義する第1の装置を設け、該第1の自動定義装置は、前記第1の計算装置の前記予め定めたアルゴリズムに前記第1の動的変数を自動的に使用できるようにする装置を含み、

前記予め定めたアルゴリズムに従って第2の予測不能コードを計算する第2の装置を設け、前記第2の計算装置は、前記一義的な静的変数を前記予め定めたアルゴリズムに対して入力する第2の装置を含み、

前記第2の入力装置が付勢される時間間隔に従って第2の動的変数を自動的に定義する第2の装置を設け、該第2の自動定義装置は、前記第2の計算装置の前記予め定めたアルゴリズムに前記第2の動的変数を自動的に使用できるようにする装置を含み、

前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を設けることを特徴とする装置。

(18) 前記第1の計算装置が、前記予め定めたアルゴリズムを実施する第1のプログラムをロードされた第1のコンピュータを含むことを特徴とする特許請求の範囲第17項記載の装置。

(19) 前記第1のコンピュータが、前記第1のプログラムを動作装置と共に内蔵された揮発性の動的メモリーに格納し、前記動作装置は、侵込みされた時、少なくとも前記プログラムと前記静的変数とを含む全てのデータを破壊することを特徴とする特許請求の範囲第18項記載の装置。

(20) 前記第1の動的変数を自動的に定義する前記第1の装置が、前記予め定めたアルゴリズムに前記第1の動的変数を自動的に使用できるようにして、前記静的変数が入力される時間間隔に従って前記第1の動的変数を定義する時計装置を含むことを特徴とする特許請求の範囲第19項記載の装置。

(21) 前記第2の計算装置が、前記第1のコンピュータから離れた接近管理装置を含み、該接近管理装置は、前記予め定めたアルゴリズムを実施する第2のプログラムをロードされていることを特徴とする特許請求の範囲第20項記載の装置。

(22) 前記第2の動的変数の自動定義装置が、前記接近管理装置の前記予め定めたアルゴリズムに前記第2の動的変数を自動的に使用可能にして、前記静的変数が入力される前記時間間隔に従って前記第2の動的変数を定義する時計装置を含むことを特徴とする特許請求の範囲第21項記載の装置。

(23) 前記第2のプログラムが動作装置と共に内蔵された揮発性の動的メモリーに維持され、前記動作装置は、侵込みされた時、前記プログラムと前記第2のプログラムに入力される静的変数とを含む全てのデータを破壊することを特徴とする特許請求の範囲第21項又は第22項記載の装置。

(24) 前記第2の計算装置と前記比較装置とに対する前記静的変数および前記第1の予測不能コードの即時の順次通信をそれぞれ行なう装置を更に設けることを特徴とする特許請求の範囲第17項記載の装置。

(25) 前記第2の計算装置と前記比較装置とに対する前記静的変数および前記第1の予測不能コードの即時の順次通信をそれぞれ行なう装置を更に設けることを特徴とする特許請求の範囲第21項記載の装置。

(28) 前記第2の計算装置が、前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を含むことを特徴とする特許請求の範囲第24項記載の装置。

(27) 前記第2のの計算装置が、前記第1の予測不能コードを前記第2の予測不能コードと比較する装置を含むことを特徴とする特許請求の範囲第25項記載の装置。

(28) 前記第1のコンピュータと前記第1の自動定義装置とが、クレジット・カードと略々同じサイズのカードに内蔵されることを特徴とする特許請求の範囲第19項、第21項、第24項又は第25項のいずれかに記載の装置。

(29) 前記接近管理装置が携帯可能であることを特徴とする特許請求の範囲第22項記載の装置。

(30) 前記静的変数を前記第1のコンピュータの予め定めたアルゴリズムに対して自動的に入力する装置を更に設けることを特徴とする特許請求の範囲第19項記載の装置。

(31) 前記第1の予測不能コードを個々に検出する装置を更に設けることを特徴とする特許請求の範囲第30項記載の装置。

(32) 予測不能コードを生成して比較する方法において、

静的変数を予め定めたアルゴリズムを含む第1のコンピュータに対して入力し、

該第1のコンピュータの前記アルゴリズムを用いて、前記静的変数と、前記入力ステップが生じた時間間隔により定義される第1の動的変数とに基いて第1の予測不能コードを計算し、

前記静的変数を前記予め定めたアルゴリズムを独立的に含む接近管理装置に対し入力し、

前記接近管理装置のアルゴリズムを用いて、前記静的変数と前記入力ステップが生じた時間間隔により定義される第2の動的変数とに基いて、第2の予測不能コードを独立的に計算し、

前記接近管理装置のアルゴリズムを用いるステップと前記第1のコンピュータのアルゴリズムを用いるステップにおいて計算される予測不能な数字コードを比較するステップとからなり、

前記第1の動的変数と前記第2の動的変数は、前記接近管理装置のアルゴリズムを用いるステップと前記第1のコンピュータのアルゴリズムを用いるステップが同じ時間間隔内に生じる時にのみ前記アルゴリズムから整合するコードを生成するように等しいことを特徴とする方法。

(33) 前記第1のコンピュータのアルゴリズム用いるステップが、前記静的変数の前記第1のコンピュータに対する入力に応答して、前記第1の動的変数を前記第1のコンピュータのアルゴリズムに対し自動的に入力する時計装置により前記第1の動的変数を定義するステップを含むことを特徴とする特許請求の範囲第32項記載の方法。

(34) 前記第1のコンピュータが、組込みされた時前記プログラムおよび静的変数を含む全てのデータを破壊する動作装置と共に内蔵された揮発性の動的メモリーに格納された前記アルゴリズムを含む第1のプログラムを有するマイクロプロセッサを含むことを特徴とする特許請求の範囲第33項記載の方法。

(35) 前記静的変数を入力するステップが更に、前記入力ステップが生じると同じ時間間隔内で前記第1と第2の予測不能コードを比較する装置に対し前記第1の予測不能コードを通信するステップを更に含むことを特徴とする特許請求の範囲第34項記載の方法。

(36) 前記接近管理装置のアルゴリズムを用いる前記ステップが更に、前記静的変数の前記接近管理装置に対する入力に応答して、前記接近管理装置のアルゴリズムに対し前記第2の動的変数を自動的に入力する時間装置により第2の動的変数を定義するステップを含むことを特徴とする特許請求の範囲第33項又は第35項記載の方法。

(37) 前記接近管理装置のアルゴリズムを用いる前記ステップが、前記静的変数を入力する前記ステップの実施に応答して、前記第2の動的変数を前記第2のコンピュータに対して自動的に入力する時計装置により前記第2の動的変数を定義するステップを含むことを特徴とする特許請求の範囲第35項記載の方法。

(10) 前記静的変数を入力する前記ステップが、前記マイクロプロセッサにより自動的に実施されることを特徴とする特許請求の範囲第17項記載の方法。

(19) 第1の機構が、それに入力される一義的な静的変数と動的変数の双方に応答して、ある予め定めたアルゴリズムに従って第1の予測不能コードを生成し、第2の機構が、前記一義的な静的変数と前記第1の動的変数と対応する第2の動的変数との双方に応答して、前記予め定めたアルゴリズムに従って第2の予測不能コードを生成し、前記2つの予測不能コードを比較する装置を含む形式の機密保護システムにおいて使用される携帯可能な手に保持される計算機表示装置であって、第1の機構を形式する装置において、

前記アルゴリズムを内部に予めプログラムされたプロセッサと、

前記アルゴリズムを知るため前記プログラムに対する接近を行おうとすると前記プロセッサに格納された前記プログラムを消去させる装置と、

各装置内に一義的な静的変数を格納する装置とを設け、該静的変数は第2の機構と共に使用されるためのどの2つの装置も同じ静的変数を格納することがないように選択され、

時間と共に変化する動的変数を生成する装置を設け、該装置は実質的に同じ時間間隔において前記第2の機構において生成されたものと同じ動的変数を生成するようになっており、

前記格納された一義的な静的変数とその時生成された動的変数とを前記プロセッサに対して与える装置と、

前記プロセッサによりその時生成されつつある予測不能コードを視覚的に表示する装置とを設けることを特徴とする装置。

(19) 前記プロセッサを内部に密閉したクレジット・カードのサイズのカードの形態を有することを特徴とする特許請求の範囲第39項記載の装置。

(41) 前記カードが、約84mm(3.3インチ)の長さと約53mm(2.1インチ)の巾と約1.8mm(0.07インチ)より薄い厚さとを有することを特徴とする特許請求の範囲第40項記載の装置。

(42) 前記視覚的に表示する装置が液晶ディスプレイであることを特徴とする特許請求の範囲第39項記載の装置。

(43) 時間と共に変化する動的変数を生じる前記装置が電子的なクロック・ゼネレータであることを特徴とする特許請求の範囲第39項記載の装置。」

(2) 明細書の第11頁第16行目乃至第18行目を次のように補正する。「データに対する接近（以下本文では、「許可または接近」という）を得ることができないようにする必要がしばしば生じる。不当な許可または接近を」

(3) 明細書中に次のような補正を行う。

頁	行	補正前	補正後
22	3	または	または取引を
	4	対する取引を制限	制限
	16	しばしば相互に同期時期	相互に時間的同期
	17	個々の	個別の
	17	生じるデータ	発生される日付
22	18	基づいて	基づいて、
23	1-2	変更	変化
	2	何時でも与える	与える
	3	容易に	何時でも容易に
	5	なる。	ある。
	12-13	するか	したり
	13	許される	与えられる
24	6	整合	整合(突き合わせ)
	12	静的変数が	前記静的変数が前記
	17	予測	第2の予測
	19	前記の2つ以上の	2つ以上の第2の
25	11	一方に	内の一つに
	17	(全文)	変数が
	18	される	される、第2のクロック機構により定義される如き
26	4	第2の突合せする	整合する第2の
27	10	基づいて	基づいて、
	11	コードとして	コードを

37	15	のため	の検出のため
38	1	基づいて	基づいて、
	7	生じる	生じた
	9、11	揮発姓	揮発性
	10	コンピュータ	プロセッサ
	13	生じる	生じた
	16	整合する	整合するような、
	17	個々の	個別の
39	1	方法も	方法が
	10	一方に	内の一つに

(4) 明細書の第38頁第4行目乃至第6行目を次のように補正する。

「タのアルゴリズムを用いて、前記静的変数と第1の時間間隔により定義される第1の動的変数に基づき第1の予測できないコードを計算」

(5) 明細書の第38頁第13行目乃至第14行目を次のように補正する。

「静的変数と第2の時間間隔の2つ以上のセルにより定義される2つ以上の動的変数に基づき2つ以上の第2の予測できないコードを独立的に」

37	3	機構、および	機構が同期され、かつ
	15	または	や、
	16	いずれか一方の	(削除)
38	4	あるいは、	即ち、
	13	または	や、
39	5	または	や、
	6	10	コード10
	11、13	揮発姓	揮発性
	13	おける	おいて
40	4	揮発姓	揮発性
	15	するも	するが
41	1	あれる	される
	3-4	揮発姓	揮発性
	8	38	38それ自体
	9	所持	入手
42	1	どれかを	どれでも
43	4	故に	故に、該
	6	偶発的	付随的

(7) 明細書の第43頁第1行目乃至第3行目を次のように補正する。

「い。メモリーへの意図的な侵入と同時に包含されたアルゴリズムを破壊する揮発性の電子的な動的メモリーにアルゴリズムが格納される」

(6) 明細書中に次のような補正を行う。

頁	行	補正前	補正後
30	5	これからある突合せる	これらからある整合する
	11	最も	整合状態の最も
	11	突合せの決定	決定
	11	選定された値により	(削除)
	19	故を	故を選定された値により
31	16、20	揮発姓	揮発性
32	15	照合	参照
33	20	個々に許可	許可
	20	ライブラリと	ライブラリと個々に
35	1	揮発姓	揮発性
	3	備え	備えた
	10	結果の	結果
36	4	結果の	結果
	18	130	130の「NO」
37	1	結果の	結果

(8) 明細書中に次のような補正を行う。

頁	行	補正前	補正後
44	11	(全文)	む。従って、別の図
	13	ついて	ついてどのアルゴリズム即ち演算も
	15	かなり	からなり
	15	ように	ために
	19	2番目の	第2の
45	1	用いられた	用いられたのと
	19	最初の	第1の
	20	2番目の	第2の
46	1	2番目	第2の
	8、11	結果の	結果
	13、15	結果の	結果
	18、19	結果の	結果
	18	用いられように	用いられるように

47	1	2番目の	第2の
	6	如く	如く、
	9	結果の	結果
48	4	440	40
49	4	1分後	1分後に
	11	2番目	第2の
	13	2番目の	第2の
	18	カード・カード・	カード・
51	2、17	結果の	結果
	8	時間	時間に対して、
	8	送れ	遅れ
53	2、5	結果の	結果
	3	間	境界
	10	取引き	手続き
33	6	2番目の	第2の
	7	間	境界
	13	結果の	結果
54	6	間	境界
	10-11	1分間格納される	1分間の格納された

54	16	それにも拘らず格納され	格納され(第3図、ステップ190)
	18	(全文)	されたエントリの時間
	20	190	130
55	4、5、10	間	境界
	20	対して	対しても
56	15	パルス	ピン
	15	間	と境界をなす
57	1	に典型的に	に
	1、3	間	境界
	10	送れ	遅れ
58	16-17	結果の	結果
59	2、6	間	境界
	4	整合する2番目の	、整合する第2の
61	2	間	境界
62	5、7、13	番号	数
63	2	番号	数
	12、16	間	境界
	18	間	境界

64	2、6、9	番号	数
64	16、19	番号	数
66	14	番号	数
67	8	間	境界
	10、18	番号	数
68	10	ものであり	であり
	11	ずを	ずれを
	14	最初の	第1の
69	6	ならばじ	ならば
	14	このように	このように、
70	8、16	揮発性	揮発性
	3-6	揮発性	揮発性
71	2	10が	10が第1の予備不能コード40を
	3	(全文)	算した後で、コー
	19	結果の	結果
72	16	第3A図及び第3B図	第3図
73	2	得る	得られる
	3	おける	おける、
73	8	30、60、60	30、60

73	10	監視装置	管理装置

以 上

手続補正書（方式）

昭和62年2月30日

特許庁長官 黒田明雄 殿

1. 事件の表示
   昭和61年 特 願第 283041 号

2. 発明の名称
   別個の時間制御装置を同期させる装置
   および方法

3. 補正をする者
   事件との関係 出願人
   住所
   名称 セキュリティ・ダイナミックス・テクノロジーズ
   インコーポレーテッド

4. 代理人
   住所 東京都千代田区大手町二丁目2番1号
   新大手町ビル 206号室
   氏名 (2770) 弁理士 鈴江孝三

5. 補正命令の日付 昭和62年2月24日（発送日）

6. 補正の対象
   出願人の代表者名を記載した願書
   委任状及訳文
   図面

7. 補正の内容
   別紙の通り

特許庁 62.5.29
特許庁 62.7.31